



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/516,236	03/01/2000	William A. Aiello	1999-0053	3274

7590 12/15/2003

Samuel H Dworetsky
AT&T Corp
P O Box 4110
Middletown, NJ 07748-4110

EXAMINER

ZIA, MOSSADEQ

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 12/15/2003

6

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/516,236

Applicant(s)

AIELLO ET AL.

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 01 March 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
- a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4, 9, 11-15, 20, 22-26, 31, 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Patent No. 5,153,919, Reeds, III et al.

3. Regarding claim 1, 23, Reeds discloses a method of provisioning a user's broadband telephony interface comprising the steps of:

Receiving the information authenticating a provisioning server (base station, Reeds, col. 3, line 21-23);

Establishing a communication channel between the user and the provisioning server over which is transmitted authorization information from the user to the provisioning server (Reeds, col. 3, line 20-24); and

Encrypting (hashing, Reeds, col. 3, line 15-16) and transmitting a cryptographic key (authentication string, Reeds, col. 5, line 60-61) associated with the user (mobile unit) to the provisioning server (Reeds, col. 3, line 15-16).

4. Regarding claims 2, 13, 24, Reeds discloses claim 1 above, and further disclose that the communication channel is a voice channel connection (Reeds, col. 9, line 35-26).

5. Regarding claims 3, 14, 25, Reeds discloses claim 2, 13, 24 above, and further disclose that the communication channel is encrypted using an audio channel key (SSD-B, Reeds, col. 6 ,

Art Unit: 2134

line 9-11, 14-16, col. 9, line 46-47) which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

6. Regarding claims 4, 15, 26, Reeds discloses claim 3, 14, 25 above, and further disclose that the cryptographic key associated with the user is encrypted using a session key (Group A and B, Reeds, col. 9, line 44-48) which is encrypted and transmitted to the provisioning server prior to establishing the communication channel.

7. Regarding claims 9, 20, 31, Reeds discloses claim 1 above, and further disclose cryptographic key associated with the user is a symmetric key (Reeds, col. 10, line 23-24).

8. Regarding claim 11, 22, 33, Reeds discloses claim 1 above, and further disclose a hash in included with each transmission (Reed, col. 12, line 48-51).

9. Regarding claim 12, Reeds discloses a broadband telephony interface comprising:
a first interface to a user telephone (mobile unit, Reeds, fig. 1, element 22, col. 4, line 20);

a second interface to a communication network (common carrier) with access to a provisioning server (base station) (Reeds, fig. 1, element 10, col. 4, line 10-11, 16-18);

memory for storing cryptographic keys (Reeds, col. 4, line 43-44);

a processor connecting to the memory and the first and second interfaces for executing program instructions, the program instructions causing the processor to perform the steps of (Reeds, fig. 11):

Receiving the information authenticating a provisioning server (base station, Reeds, col. 3, line 19-22);

Art Unit: 2134

Establishing a communication channel between the user and the provisioning server over which is transmitted authorization information from the user to the provisioning server (Reeds, col. 3, line 20-24); and

Encrypting (hashing, Reeds, col. 3, line 15-16) and transmitting a cryptographic key (authentication string, Reeds, col. 5, line 60-61) associated with the user (mobile unit) to the provisioning server (Reeds, col. 3, line 15-16).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 5-8, 10, 16-19, 21, 27-30, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,153,919, Reeds, III et al in view of "Background of the Invention" of Patent No. 5,153,919, Reeds, III et al.

12. Regarding claims 5, 16, 27, Reeds discloses claim 4, 15, 26 above but fails to clearly disclose that the session key and the audio channel key are encrypted using a cryptographic key that is encrypted using a cryptographic key associated with the provisioning server and the transmitted to the provisioning server with the encrypted session and audio channel key.

Reed's Background teaches an authentication technique when party A wishes to communicate with party B, it sends to authentication server AS his own name, the name of party B and a transaction identifier. Server AS returns the name of party B, a session key (session and

Art Unit: 2134

audio channel key), the transaction identifier and a message encrypted with B's key. All that information is encrypted with A's key. Party A receives the information, decrypts it, selects the portion that is encrypted with B's key (cryptographic key associated with the provisioning server) and forwards that portion to party B. Party B decrypts the received messages and finds the name of party A and the session key. A last check is made by party B issuing a challenge to party A and party A replies, using the session key (Reeds, col.2, line 59-68, col. 3, line 1-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Reeds as per teaching of "Background of the Invention" to include the above authentication technique to prevent replays (Reeds, col. 3, line 1-2).

13. Regarding claims 6, 17, 28, Reeds discloses claim 5, 16, 27 above and further discloses that the cryptographic key associated with the provisioning server is received with the information authenticating the provisioning server (Reeds, col. 2, line 67-68, col. 3, line 1).

14. Regarding claims 7, 18, 29, Reeds discloses claim 6 above and further discloses that a random nonce (transaction identifier) is included with the encrypted session key (Reeds, col. 2, line 63-65).

15. Regarding claims 8, 19, 30, Reeds discloses claim 1 above, but fails to disclose that the information authenticating the provisioning server is a digital certificate.

Reed's Background teaches public key cryptography where a mobile station would be provided with a public key certificate (digital certificate) of identity, signed by the public key of the service provider (provisioning server), stating that the mobile station is a legitimate customer of the service provider (Reeds, col. 2, line 20-24).

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Reeds as per teaching of "Background of the Invention" to include public key cryptography to provide another standard class of ways to for solving authentication problems (Reeds, col. 2, line 17-18).

16. Regarding claims 10, 21, 32, Reeds disclose claim 1 above, but fails to disclose that the cryptographic key associated with the user is a public key corresponding to a private key stored in the broadband telephony interface.

Reed's Background teach that mobile station using public key cryptography where it would be given secret data (private keys) which it can use, together with a certificate, to prove to third parties (such as the serving system) that it is a legitimate user (Reeds, col. 2, line 24-27).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Reeds as per teaching of "Background of the Invention" to include public key cryptography to provide another standard class of ways to for solving authentication problems (Reeds, col. 2, line 17-18).

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Art Unit: 2134

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

mz
12/9/03


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2134